Facial Recognition by the Government: Privacy and Civil Liberties Issues

Professor Peter Swire
Ohio State University & Future of Privacy Forum

FBI Biometric Center of Excellence

March 14, 2012

Two Perspectives on U.S. Government Use of Facial Recognition

- **It's Public.**
  - People are walking down the street
  - Police have always watched people in public
  - It's good to use modern information tools to do this more efficiently

Second Perspective

- **It's something new and different.**
  - The government getting real time location information of citizens off of cameras?
  - Part of my permanent record?
  - What if I am with someone "suspicious"?
  - 1972 Democratic Convention
    - Levi Guidelines, Privacy Act, FISA
  - NYC and mosques in press recently

Overview

- Constitutional issues
  - 4th Amendment and beyond
- Statutes
  - Privacy Act, Wiretaps and Stored Records
- Subset of legal actions
  - What is good to do

My Background

- Ohio State, law professor, live in DC area
- Future of Privacy Forum project now on government access to personal information
- 2009-2010, National Economic Council
- 1999-2001, Chief Counselor for Privacy, OMB
  - WH Working Group to update wiretap laws
  - Privacy Act
- Security and privacy
  - Manhattan DA

Constitutional Issues

- Fourth Amendment (search)
- First Amendment (speech, association)
- Fourteenth Amendment (anti-discrimination)
- Due Process

- For each:
  - Doctrine, and legal prohibitions
  - Values, sensitivities, public concerns

4th Amendment

- Warrant, with probable cause
  - No unreasonable searches or seizures
  - Clear limits on entering an individual's house, car, etc.
  - Observing a person in public, though, hasn't required a search warrant to see

“In Public”

- Major reason that may be OK for government to do facial recognition
  - Can follow an individual down the street
  - Can read newspapers & other public documents
  - Not a “search” or “seizure”
  - A foundation of DOJ/DHS actions for years

Jones GPS Case & “In Public”

- Supreme Court, 9-0, said warrant needed to put a GPS tracker on a car
  - Car “in public”
  - Majority emphasized physical attachment
  - Four or five justices questioned whether “in public” is enough to make surveillance OK
  - “Mosaic” theory and what are the limits on government surveillance

Alito in Jones (4 votes)

- Would find a “search” for observing a car “in public”
- “Society’s expectation has been that l.e. agents and others would not – and indeed, in the main, simply could not – secretly monitor and catalogue every single movement of an individual’s car for a very long period”
- “the line was surely crossed before the 4-week mark”
- Reasonable expectation of privacy, so need a warrant
- Sotomayor (5th vote) may agree, but she wrote separately

Montana Supreme Court

- State investigators secretly videotaped a worker's comp claimant around town
- State argued "a person has no privacy expectation for what he or she does in plain view in public"
- 2 judges cited *Jones*: "We do not accept cameras that follow us all around town, monitoring and recording our every move for no purpose other than to detect and document evidence of unlawful activity."
- "Montanans do retain expectations of privacy while in public."
- *Montana State Fund v. Simms*

"Consent" Exception to 4th Am.

- Another foundation of 4th Am: individual can consent to a search or seizure
  - You can agree to have the cop enter your house
- Person voluntarily is walking down the street
- Or, voluntarily is at the bank or the mall, where cameras are
- So, consent has been given?

Was It Really Consent?

- Consent to surveillance "in public"?
  - Often no actual knowledge or consent
  - Question is when to find "implied consent"
  - Alito questions that for long-term tracking
- Consent to surveillance by private actors?
  - "Third party doctrine"
    - You consented to banks reading your checks
    - You consented to phone companies keeping to/from information

Third Party Doctrine

- Sotomayor: “More fundamentally, it may be necessary to reconsider the premise that an individual has no REP in information voluntarily disclosed to third parties”
- “This approach is ill suited to the digital age”
- She cites *Katz*: “What a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected”
- Many scholars agree – is it really “consent” to the government when your cell phone provider learns the numbers you call?

Wrap-Up on 4th Amendment

- Jones appears to be a Big Deal
  - What can be done "in public"
  - What counts as "consent" to surveillance
- DOJ treating it as a Big Deal
  - Thousands of GPS devices halted
  - Policy review
- Solove proposal: "The Fourth Amendment applies to a surveillance technology used in public if the surveillance technology: (1) extends significantly beyond human capabilities; and (2) is used in a manner beyond its ordinary use by the general public."
- Drones and Jones

First Amendment

- Sotomayor: “Awareness that the Government may be watching chills associational and expressive freedoms.”
- Location -- “a wealth of detail about her familial, political, professional, religious, and sexual associations”
- NAACP v. Alabama – protection of private list of members of a political association
- Democratic convention, 1972

Due Process/Accountability

- Risk – if have databases with pervasive data on citizens, then discretion & power to those who access the database
  - Importance of accountability, audits, due process
  - Penalties for "peeping"
- Sobriety stops – must have procedures
- Minimization of wiretaps – procedures
- Swire Stanford article on "in accordance with law" for 4th Amendment

Equal Protection

- Great caution about discrimination based on religion, race, politics, ethnic origin, etc.
- Britain: blacks 150% to 250% rate of surveillance of whites from CCTV
  - "Walking while black?"
- Elevator videos in Britain – gender
- DC case of police officer charged with using databases to blackmail married patrons of gay establishments

Statutes: The Privacy Act

- Privacy Act of 1974
  - Agency, such as DHS, issues a System of Records Notice, in Federal Register
  - SOR where information "is retrieved" by name or identifier
  - Used within that agency, without need for consent
  - Lists the "routine uses" where goes to other agencies

Privacy Act

- Variety of safeguards on the data
- Privacy Act data subject to access requests by the individual – “what do you have on me?”
- Limit on data about exercise of rights guaranteed by the First Amendment, unless within scope of l.e. activity
- Major law enforcement exceptions

PII

- Privacy Act applies to “personally identified information”
  - “identified” or “identifiable”
  - Not much OMB guidance on that
- Census & long tradition of masking data
- HIPAA and “deidentified data”
  - Mask 18 specified data fields; or
  - Expert witness that “very low” chance of reidentifying

One Federal Statute

- Federal Video Voyeurism Prevention Act of 2004
  - Ban on knowingly capturing an image of the "private area" of an individual
  - Where reasonable person would believe can disrobe in privacy
  - Applies only on federal lands
  - Similar state laws

Statutes: Wiretaps

- Strict limits on government interception of phone calls and bugging for sound (Title III)
  - Extra-strict search warrant
  - **Content** of private communications very sensitive
- Applies to "aural"
  - **Not** to video only

Statutes: Stored Communications

- Stored Communications Act applies to records held by a third party
  - Would apply if you subpoena FB for photos and/or names
- Medium level of strictness to get data
- Shows medium level of sensitivity for content of stored records

Current Mystery: Location Information

- Split in lower courts now whether need a warrant to get a person's cell phone location information
- Big battle brewing
- Sensitivity of location
  - Cell phone and track a person in unprecedented ways
  - Pictures posted to Net often have time/date/place
- Precedents for cell phone location may predict doctrine for facial recognition location

Information Sharing

- Not focus today – the information sharing environment
- Article on privacy & information sharing in the war against terrorism
  - Check list of questions, ODNI
  - Cost effective? Security theater?
  - Lessons from history?
  - Make security problems worse?
  - International ramifications?

Subset of What is Legal

- Not everything legal is good to do
  - You know this – you teach it to your kids
- Current DHS self-restraint on social media
  - Basically, monitor public officials and traditional media types on social media
  - Careful not to track individuals
  - FBI tracking words (bomb) but not people
- That didn't prevent painful hearing last month

Tests for What is Good to Do

- Friends and family test
- New York Times test
- Data minimization:
  - Facial detection v. facial recognition

Conclusion

- Achieve these goals
  - Follow the constitution and the law
  - Do what is good to do
  - Be alert to the risk of undermining a good program by creeping people out

- **And**
  - Use new tech effectively

Some Sources

- Swire, "Privacy and Information Sharing in the War Against Terrorism," http://ssrn.com/abstract=899626
- Constitution Project, "Guidelines for Public Video Surveillance," 2007, www.constitutionproject.org
- Swire, "A Reasonableness Approach to Searches After the Jones GPS Tracking Case", http://www.stanfordlawreview.org/online/privacy-paradox/searches-after-jones

Sources

- Swire, “Peeping”, http://ssrn.com/abstract=1418091